(56) **References Cited**

U.S. PATENT DOCUMENTS

2008/0288781	A1	11/2008	Lawson et al.	
2008/0307235	A1*	12/2008	Keohane	G06F 21/46 713/183
2009/0150677	A1*	6/2009	Vedula	G06F 21/46 713/183
2009/0150971	A1*	6/2009	Vedula	G06F 21/31 726/1
2010/0299727	A1	11/2010	More et al.	
2011/0252243	A1	10/2011	Brouwer et al.	
2011/0314294	A1*	12/2011	McGrew	G06F 21/46 713/182

OTHER PUBLICATIONS

Glodek, William, "Using a Specialized Grammar to Generate Probable Passwords" (2008). Electronic Theses, Treatises and Dissertations. Paper 4238.*

Weir et al., Testing metrics for password creation policies by attacking large sets of revealed passwords. Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10). Chicago, Illinois. 2010: 162-175.

Verheul. Selecting secure passwords. Topics in Cryptology—CT-RSA 2007: M. Abe (Ed.) 2007. Lecture Notes in Computer Science. 4377: 49-66.

Stone-Gross et al., Your botnet is my botnet: Analysis of a botnet takeover. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09). Chicago, Illinois. 2009: 635-347.

Shay et al., Encountering stronger password requirements: user attitudes and behaviors. 6th Symposium on Usable Privacy and Security (SOUPS). Redmond, WA. 2010: 1-20.

Riley. Password security: what users know and what they actually do. Usability News. 2006. vol. 8 (No. 1): 1-5.

Furnell. An assessment of website password practices. Computers & Security. 2007. vol. 26: 445-451.

Burr et al., NIST special publication 800-63-1 electronic authentication guideline. National Institute of Standards and Technology. U.S. Department of Commerce. Gaithersburg, MD. 2011: 1-121.

Zhang et al., The security of modern password expiration: an algorithmic framework and empirical analysis. Proceedings of 17th ACM Conference on Computer and Communication Security (CCS '10). Chicago, Illinois. 2010:176-186.

Inglesant and Sasse. The true cost of unusable password policies: password use in the wild. CHI 2010: Privacy Behavior. Atlanta, Georgia. 2010: 383-392.

Charoen et al., Improving end user behavior in password utilization. Systemic Practice and Action Research. 2008. vol. 21: 55-72.

Adams and Sasse. Users are not the enemy. Communications of the ACM. 1999. vol. 42 (No. 12): 40-46.

Campbell et al., Impact of restrictive composition policy on user password choices. Behavior and information technology. 2011. vol. 30 (No. 3): 379-388.

Florencio and Herley. A large-scale study of web password habits. Proceeding of the 16th Int. Conf. on World Wide Web (WWW '07). Track: Security, Privacy, Reliability, and Ethics. Session: Passwords and Phishing. Banff, Alberta, Canada. 2007: 657-665.

Komanduri et al, Of passwords and people: measuring the effect of password-composition policies. Proceeding the SIGCHI Conference on Human Factors in Computing Systems (CHI '11). Session: Authentication. Vancouver, BC, Canada. 2011: 2595-2604.

Bard. Spelling-error tolerant, order independent pass-phrases via the Damerau-Levenshtein string-edit distance metric. Proceedings of the Fifth Australasian Symposium on ACSW Frontiers. Ballarat, Australia. 2007. vol. 68: 117-124.

Yan et al., The memorability and security of passwords—some empirical results. Technical Report No. 500. Computer Laboratory, University of Cambridge. 2000: 1-11.

Forget et al., Improving text passwords through persuasion. Symposium on Usable Privacy and Security (SOUPS). Pittsburgh, PA. 2008: 1-12.

Yan. A note on proactive password checking. Proceedings of the 2001 workshop on New Security Paradigms (NSPW '01). Cloudcroft, New Mexico. 2001: 127-135.

Spafford. OPUS: preventing weak password choices. Computers& Security. 1992. vol. 11: 273-278.

Schetcher et al., Popularity is everything: a new approach to protecting passwords from statistical-guessing attacks. HotSec'10: Proceedings of the 5th USENIX conference on Hot Topics in Security. 2010: 1-6.

Castelluccia et al., Adaptive password-strength meters from Markov models. NDSS '12. 2012.

Weir et al., Password Cracking Using Probabilistic Context Free Grammars. Proceedings of the 30th IEEE Symposium on Security and Privacy. 2009: 391-405.

Shannon. Prediction and entropy of printed English. Bell Systems Tech. J. 1951. vol. 30: 50-64.

Massey. Guessing and entropy. 1994 IEEE Symposium on Information Theory. 1994: 204.

Damerau. A technique for computer detection and correction of spelling errors. Communications of the ACM. 1964. vol. 7 (No. 3): 171-176.

Vance. If your password is 123456, just make it hackme. New York Times. 2010. Date Accessed Sep. 2, 2014. http://www.nytimes.com/2010/01/21/technology/21password.html.

Warren. Thousands of Hotmail Passwords Leaked. 2009. Date Accessed Sep. 2, 2014. http://www.neowin.net/news/main/09/10/05/thousands-of-hotmail-passwords-leaked-online.

The Open wall group,.John the Ripper password cracker. Date Accessed Jul. 30, 2014. http://www.openwall.com/john/.

A list of popular password cracking wordlists. 2005. Date Accessed Sep. 2, 2014. http://www.outpost9.com/files/WordLists.html.

McMillan. Phishing attack targets MySpace users. 2006. Date Accessed Sep. 2, 2014. http://www.infoworld.com/d/security-central/phishing-attack-targets-myspace-users-614.

Morris and Thompson. Pasword security: a case history. Communications of the ACM. 1979. vol. 22 (No. 11): 594-597.

Weir. Using Probabilistic Techniques to aid in Password Cracking Attacks. Dissertation. Florida State University. 2010: 1-140.

Booth and Thompson. Applying Probability Measures to Abstract Languages. IEEE Transactions on Computers. vol. C-22 (No. 5). 1973: 442-450.

Kuo et al., Human Selection of Mnemonic Phrase-based Passwords. Symp. on Usable Privacy and Security (SOUPS). 2006: 1-12.

Monrose et al., Password hardening based on keystroke dymanics. ACM Conference on Computer and Communications Security. CCS. 1999: 73-82.

Manber. A simple scheme to make passwords based on one-way functions much harder to crack. Computer & Security. 1996. vol. 15 (No. 2): 171-176.

Sophos. Security at risk as one third or surfers admit they use the same passwords for all websites. 2009. Date Accessed Jul. 30. 2014. http://www.sophos.com/pressoffice/news/articles/2009/03/password-security.html.

Stanton et al., An analysis of end user security behaviors. Computers & Security. 2005. vol. 24: 124-133.

Google. Creating a strong password. Accounts Help. Date Accessed Jul. 30, 2014. https://support.google.com/accounts/answer/32040?rd=1.

Cachin. Entropy Measures and Unconditional Security in Cryptography. PhD Thesis. Swiss Federal Institute of Technology Zurich. ETH Disseratation. No. 12187. 1997: 1-155.

Shannon. A Mathematical Theory of Communication. Bell System Technical Journal. 1948. vol. 27 (No. 3): 379-423, 623-656.

Windows. Tips for creating a strong password. Date Accessed Sep. 4, 2014. http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password.

International Search Report and Written Opinion for PCT/US2012/062730 (filing date: Oct. 31, 2012) with a mailing date of Aug. 23, 2013; Applicant: The Florida State University Research Foundation, Inc. et al.